

Docket No.: P-163

D. J.
#4 7-18-01
Priority Papers
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Yoon-Taek JUNG and Sung-Kyun PARK

Serial No.: New U.S. Patent Application

Filed: January 2, 2001

For: METHOD FOR PROCESSING AUTHENTICATION
FAILED/AUTHORIZATION DENIED SUBSCRIBERS BY INTELLIGENT
NETWORK

jc914 U.S. PTO
09/750909
01/02/01

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Assistant Commissioner of Patents
Washington, D. C. 20231

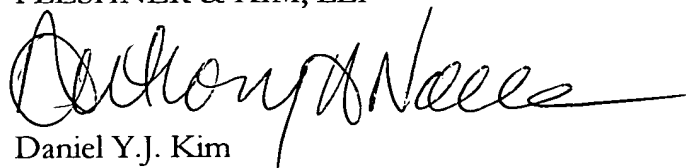
Sir:

At the time the above application was filed, priority was claimed based on the
following application:

Korean Patent Application No. 65894/1999, filed December 30, 1999.

A copy of each priority application listed above is enclosed.

Respectfully submitted,
FLESHNER & KIM, LLP



Daniel Y.J. Kim
Registration No. 36,186
Anthony H. Nourse
Registration No. 46,121

P. O. Box 221200
Chantilly, Virginia 20153-1200
703 502-9440
Date: January 2, 2001
DYK:AHN/cam

대한민국 특허청
KOREAN INDUSTRIAL
PROPERTY OFFICE

Jc914 U.S. PTO
09/750909
01/02/01

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Industrial
Property Office.

출원번호 : 특허출원 1999년 제 65894 호
Application Number

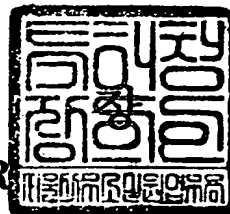
출원년월일 : 1999년 12월 30일
Date of Application

출원인 : 엘지정보통신주식회사
Applicant(s)

2000 년 10 월 09 일

특 허 청

COMMISSIONER



【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0005
【제출일자】	1999. 12. 30
【발명의 명칭】	인증 실패/권한 부정 가입자에 대한 지능망적 처리방법
【발명의 영문명칭】	Method For Intelligent Network Processing Of Authentication Failure or Authorization Denied Subscriber
【출원인】	
【명칭】	엘지정보통신 주식회사
【출원인코드】	1-1998-000286-1
【대리인】	
【성명】	김영철
【대리인코드】	9-1998-000040-3
【포괄위임등록번호】	1999-010680-1
【발명자】	
【성명의 국문표기】	박성균
【성명의 영문표기】	PARK, Sung Kyun
【주민등록번호】	690611-1037618
【우편번호】	121-210
【주소】	서울특별시 마포구 서교동 395-113
【국적】	KR
【발명자】	
【성명의 국문표기】	정윤택
【성명의 영문표기】	JUNG, Yoon Taek
【주민등록번호】	580815-1023119
【우편번호】	431-053
【주소】	경기도 안양시 동안구 비산3동 245 뉴타운아파트 9-1005
【국적】	KR
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대 리인 철 (인) 김영

1019990065894

2000/10/1

【수수료】

【기본출원료】 20 면 29,000 원

【가산출원료】 26 면 26,000 원

【우선권주장료】 0 건 0 원

【심사청구료】 0 항 0 원

【합계】 55,000 원

【요약서】**【요약】**

통신망 서비스에서 가입자가 호 발신을 시도하였을 때 가입자의 어떤 이유로 인하여 인증에 실패하거나 권한이 부정된 경우 고객센터 또는 해당 단말기의 가입자가 지정한 적법한 전화번호로 통화를 연결하거나 정상적인 호 처리를 진행하여 해당 가입자에 대한 신원파악과 적법성 여부의 판단, 상황에 따른 적절한 음성 안내 서비스의 제공 및 고객센터 담당자와의 통화 연결을 통해 정상적인 서비스로의 인도를 제공하도록 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법에 관한 것이다.

본 발명은 지능망 규격에서 호 발신을 시도한 가입자에 대한 인증이 실패하거나 권한이 부정되는 경우 해당 사실을 SCP에 통보하고, 상기 SCP에서 지시하는 바에 따라 해당 처리 동작을 수행시키는 발신호 권한 부정 감지점을 더 포함하는 것을 특징으로 한다.

따라서, 통신 서비스 망에서 가입자 발신호에 대하여 인증 실패 혹은 권한 부정된 경우 효과적인 조치 및 서비스를 다양하게 제공하며, 불법으로 복제하여 사용하는 단말기를 검출하여 적법한 가입자의 피해를 방지하여 주며, 인증에 실패하거나 권한 부정된 가입자의 호에 대한 추적 및 이력 유지가 자동으로 가능하도록 한다.

【대표도】

도 5

【명세서】**【발명의 명칭】**

인증 실패/권한 부정 가입자에 대한 지능망적 처리방법{Method For Intelligent Network Processing Of Authentication Failure or Authorization Denied Subscriber}

【도면의 간단한 설명】

도 1은 종래의 통신망 서비스에서 단말기의 발신호에 대하여 인증 실패시 발신호를 해제하는 단말기와 교환 시스템간의 흐름도.

도 2는 종래의 지능망에서 WIN 규격에 따라 발신호 처리 흐름을 보인 기본 호 상태 모델도.

도 3은 종래의 지능망에서 ITU-T 규격에 따라 발신호 처리 흐름을 보인 기본 호 상태 모델도.

도 4는 종래의 지능망에서 CAMEL 규격에 따라 발신호 처리 흐름을 보인 기본 호 상태 모델도.

도 5는 본 발명에 따른 지능망에서 WIN 규격에 따라 발신호 처리 흐름을 보인 기본 호 상태 모델도.

도 6은 본 발명에 따른 ITU-T 규격에 따라 발신호 처리 흐름을 보인 기본 호 상태 모델도.

도 7은 본 발명에 따른 CAMEL 규격에 따라 발신호 처리 흐름을 보인 기본 호 상태 모델도.

도 8은 본 발명에 따른 WIN 규격의 통신망 서비스에서 발신호의 인증 실패 및 권한 부정시 단말기와 교환 시스템간의 호 연결 서비스의 흐름도.

도 9는 본 발명에 따른 ITU-T 규격의 통신망 서비스에서 발신호의 인증 실패 및 권한 부정시 단말기와 교환 시스템간의 호 연결 서비스의 흐름도.

도 10은 본 발명에 따른 CAMEL 규격의 통신망 서비스에서 발신호의 인증 실패 및 권한 부정시 단말기와 교환 시스템간의 호 연결 서비스의 흐름도.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<11> 본 발명은 이동 통신망 서비스 제공방법에 관한 것으로, 더 상세하게는 통신망 서비스에서 가입자가 호 발신을 시도하였을 때 가입자의 어떤 이유로 인하여 인증에 실패하거나 권한이 부정된 경우 고객센터 또는 해당 단말기의 가입자가 지정한 적법한 전화번호로 통화를 연결하거나 정상적인 호 처리를 진행하여 해당 가입자에 대한 신원파악과 적법성 여부의 판단, 상황에 따른 적절한 음성 안내 서비스의 제공 및 고객센터 담당자와의 통화 연결을 통해 정상적인 서비스로의 인도를 제공하도록 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법에 관한 것이다.

<12> 일반적으로, 통신 서비스망에서는 가입자에 대한 적법성 여부를 판단하기 위하여 인증(Authentication) 기능을 사용하고 있으며, 또한 서비스 사용료에 대한 체불 등에

의하여 가입자의 서비스 권한을 금지시킬 필요성에 대비하여 가입자에 대한 권한부여 (Authorization) 기능을 사용하고 있다.

<13> 특히 이동 통신 서비스망에서는 단말기가 서비스 망과 물리적으로 분리되어 있어 단말기의 분실 또는 도난 가능성이 있으며 혹은 적법한 가입자의 단말기를 타인이 불법으로 복제하여 사용할 수 있으므로 이러한 문제점을 해결하기 위하여 이동 통신 서비스 망에서는 발신호를 요구하는 가입자에 대하여 인증 기능과 권한 부정(Authorization Denied) 기능이 적극적으로 도입되고 있다.

<14> 그러나, 발신호 요구되는 단말기에 대하여 인증에 실패한 경우에는 그 단말기를 사용하고 있는 가입자에 대한 신원 파악과 적법성 여부의 판단 등에 대한 적적할 조치가 필요하며, 분실되거나 도난 당한 단말기를 사용함으로써 권한이 부정된 경우에도 해당 단말기를 사용하고 있는 가입자에 대한 신원 파악 및 적절한 조치가 필요하다.

<15> 또한, 가입자가 서비스 사용료의 체불로 인하여 권한이 부정된 경우에도 일정 기간 동안은 적절한 음성 안내와 함께 정상적인 호 서비스를 제공하고 이후에 서비스 중단을 안내하는 방송을 하거나 혹은 서비스 망의 고객 담당자와 통화를 연결하여 정상적인 서비스로의 유도가 필요하며, 가입자가 어떠한 이유에 의하여 인증에 실패하거나 권한이 부정된 경우에도 상황에 따라서는 가입자에게 적절한 음성 안내를 해 주거나 정상적인 호 서비스를 제공해 주어야 하고, 가입자가 적법한 경우라도 어떠한 이유에 의해 인증에 실패할 수 있으므로 이 경우 해당 가입자에 대하여 정상적인 서비스를 즉각적으로 제공하여야 한다.

<16> 그러나 기존의 통신 서비스망에서는 발신호에 대한 가입자 인증이 실패하거나 권한이 부정된 경우에는 해당 가입자에 대하여 서비스의 제공을 무조건 차단하도록 되어 있

어 해당 가입자에 대한 신원 파악이나 적법성 여부의 판단, 상황에 적절한 다양한 음성 안내 혹은 정상적인 호 서비스의 제공, 해당 가입자와 고객센터의 서비스 담당자와 통화를 통한 정상적인 서비스로의 유도 등이 제공되지 않고 있다.

<17> 종래의 이동 통신 서비스 망에서 가입자의 발신호를 처리하는 동작을 도 1을 참조하여 설명하면 다음과 같다.

<18> 임의의 가입자 단말기(1)가 자신의 단말기에 대한 정보를 포함하여 이동 교환 시스템(MSC/VLR) 이나 유선 교환 시스템/SSP측에 호 발신을 요구하면(S10) 이동 교환 시스템(MSC/VLR) 이나 유선 교환 시스템/SSP는 발신호 요구되는 단말기의 정보를 분석하여 인증 및 권한 여부를 판단한 다음(S11) 적법한 단말기로부터의 발신호이면 상대방의 전화번호를 분석하여 호 설정을 시도하고, 발신호 단말기(1)에 대하여 인증에 실패되거나 권한이 부정된 단말기로부터의 발신호인 것으로 판단되면 교환 시스템에서 제공되는 단순한 안내 음성 메시지를 발신호 요구한 단말기(1)측에 송출한 다음 해당 호에 대한 서비스를 즉각적으로 중단한다(S12).

<19> 상기와 같이 인증 실패나 권한 부정된 가입자에 대한 서비스는 지능망에서도 동일하게 이루어지는데, 이에 대하여 설명하면 다음과 같다.

<20> 먼저, 도 2를 참조하여 WIN(Wireless Intelligent Network) 규격에서 정의한 발신호에 대하여 기본 호 상태 모델(Basic Call State Model)을 참조하여 설명하면 다음과 같다.

- <21> 단말기의 발신호가 호 처리점(PIC1)에 검출되면 해당 호 처리점(PIC1)은 검출되는 발신호에 대하여 이벤트 처리를 수행한 다음 지능망 서비스를 위해 다음 단계로 천이시킨다.
- <22> 호 처리점(PIC2)은 발신호에 대하여 정상적인 가입자 단말기로부터의 발신호 인지의 여부를 판단하기 위하여 인증 절차와 권한 여부를 검사하여 정상적인 가입자 단말기로부터의 발신호 인것으로 판단되어 인증과 권한이 부여되는 경우 다음 단계로 천이한다.
- <23> 호 처리점(PIC3)은 해당 발신호에 포함된 초기 정보, 즉 서비스 코드와 국번 및 착신번호에 대한 정보를 수집하며, 정보 수집에 할당된 시간이 경과하게 되는 경우 예외 처리를 수행하여 초기화 루틴으로 리턴되고, 설정된 시간 내에서 발신호에 대한 정보가 정상적으로 수집되면 다음 단계로 천이한다.
- <24> 제3감지점(DP3)에서 수집된 정보에 대한 감지점 처리가 수행된 후, 호 처리점(PIC4)을 통해 수집된 정보를 분석하며, 분석되는 정보가 호 설정을 수행할 수 없는 비가용한 정보인 경우 예외 처리를 수행하여 초기화 루틴으로 리턴되고, 가용한 발신호에 대하여 정보의 분석이 완료되면 다음 단계로 천이한다.
- <25> 제4감지점(DP4)에서 분석된 정보에 대한 감지점 처리가 수행된 후, 호 처리점(PIC5)을 통해 호 설정하고자 하는 루트를 선택한 다음 호 처리점(PIC6)을 통해 선택된 루트로 상기 인증된 발신호에 대하여 호 설정 수행하는 셋업 처리를 실행한다.
- <26> 상기 호 처리점(PIC6)에서 선택된 루트의 장애 발생이 제5감지점(DP5)에 검출되면 예외 처리를 수행시켜 초기화 루틴으로 리턴되고, 인증된 발신호에 대하여 셋업 처리에

장애가 발생하는 경우 예외 처리를 수행하여 초기화 루틴으로 리턴된다.

<27> 상기에서 호 설정에 대한 셋업이 정상적으로 수행되면 호 처리점(PIC7)을 통해 해당하는 착신측으로의 호출처리를 수행한 다음 호 처리점(PIC8)을 통해 링백톤(Ring Back Tone) 송출 및 착신 응답 대기 루틴과 호 처리점(PIC9)를 통해 발신호의 활성화 처리 루틴 및 호 처리점(PIC10)을 통해 발신호의 중단 처리 루틴을 수행한다.

<28> 상기에서 각 호 처리점의 루틴에서 장애가 검출되는 경우 해당 처리 동작에 대하여 예외 처리 루틴을 수행한 다음 초기화 루틴으로 리턴되고, 발신호의 중단이 검출되는 경우 초기화 루틴으로 리턴된다.

<29> 또한, 상기 제1감지점(DP1)에서 검출되는 발신호에 대하여 호 처리점(PIC2)에서 해당 발신호에 대하여 인증 실패 또는 권한 부여가 거부되는 경우 호 서비스의 진행을 중단하고, 예외 처리를 수행한 다음 초기화 루틴으로 리턴된다.

<30> 다른 예로 ITU-T의 권고안에 제시된 발신호에 대한 기본 호 상태 모델(BCSM)을 참조하여 설명하면 다음과 같다.

<31> 단말기의 발신호가 호 처리점(PIC21)에 검출되면 해당 호 처리점(PIC21)은 검출되는 발신호에 대하여 이벤트 처리를 수행한 다음 지능망 서비스를 위해 다음 단계로 천이시킨다.

<32> 호 처리점(PIC22)은 발신호에 대하여 정상적인 가입자 단말기로부터의 발신호 인지의 여부를 판단하기 위하여 인증 절차와 권한을 검사하여 정상적인 가입자 단말기로부터의 발신호 인것으로 판단되어 인증과 권한이 부여되는 경우 다음 단계로 천이한다.

- <33> 호 처리점(PIC23)은 해당 발신호에 포함된 초기 정보, 즉 서비스 코드와 국번 및 착신번호에 대한 정보를 수집하며, 정보 수집에 할당된 시간이 경과하게 되는 경우 예외 처리를 수행하여 초기화 루틴으로 리턴되고, 설정된 시간 내에서 발신호에 대한 정보가 정상적으로 수집되면 다음 단계로 천이한다.
- <34> 제3감지점(DP23)에서 수집된 정보에 대한 감지점 처리가 수행된 후, 호 처리점(PIC24)을 통해 수집된 정보를 분석하며, 분석되는 정보가 호 설정을 수행할 수 없는 비가용한 정보인 경우 예외 처리를 수행하여 초기화 루틴으로 리턴되고, 가용한 발신호의 대한 정보의 분석이 완료되면 다음 단계로 천이한다.
- <35> 제4감지점(DP24)에서 분석된 정보에 대한 감지점 처리가 수행된 후, 호 처리점(PIC25)을 통해 호 설정을 위한 루트를 선택한 다음 호 처리점(PIC26)을 통해 선택된 루트로 인증된 발신호에 대하여 호 설정 셋업 처리를 실행한다.
- <36> 상기에서 제5감지점(DP25)에 선택된 루트의 장애가 검출되면 예외 처리를 수행하여 초기화 루틴으로 리턴되고, 인증된 발신호에 대하여 셋업 처리에 장애가 발생하는 경우 예외 처리를 수행하여 초기화 루틴으로 리턴된다.
- <37> 상기에서 호 설정에 대한 셋업이 정상적으로 수행되면 호 처리점(PIC27)을 통해 해당하는 착신측으로의 호출처리를 수행한 다음 호 처리점(PIC28)을 통해 링백톤 송출 및 착신 응답 대기 루틴과 호 처리점(PIC29)를 통한 발신호의 활성화 처리 루틴 및 호 처리점(PIC30)을 통한 발신호의 중단 처리 루틴을 수행한다.
- <38> 상기에서 각 호 처리점의 처리 루틴에서 장애가 발생하는 경우 예외 처리 루틴을 수행한 다음 초기화 루틴으로 리턴되고, 발신호의 중단이 검출되는 경우 초기화 루틴으

로 리턴된다.

<39> 또한, 제1감지점(DP21)에서 검출되는 발신호에 대하여 호 처리점(PIC22)에서 해당 발신호에 대하여 인증 실패 또는 권한 부여가 거부되는 경우 호 서비스의 진행을 중단하고, 예외 처리를 수행한 다음 초기화 루틴으로 리턴된다.

<40> 또 다른 실시예로 도 4를 참조하여 CAMEL(Customised Applications for Mobile network Enhanced Logic)에서 정의한 발신호에 대하여 기본 호 상태 모델(BCSM) 참조하여 설명하면 다음과 같다.

<41> 호 처리점(PIC41)에 발신호에 대한 이벤트가 검출되면 해당 발신호에 대한 인증과 권한 여부 및 발신호에 대한 초기 정보 등을 검출하여 해당 발신호 처리를 위하여 정보의 분석을 요구한다.

<42> 제1감지점(DP41)에서 수집된 정보에 대한 감지점 처리가 수행된 후, 호 처리점(PIC42)을 통해 발신호에 대하여 수집된 정보의 분석을 수행하여 해당 정보가 비가용한 정보인 경우 예외 처리를 수행한 다음 초기화 루틴으로 리턴되고, 가용한 정보인 것으로 판단되면 다음 단계로 천이한다.

<43> 제2감지점(DP42)에서 분석된 정보에 대한 감지점 처리가 수행된 후, 호 처리점(PIC43)에서는 발신호의 루팅 요구에 따라 호 설정을 위한 루트를 선택한 다음 호 설정 메시지를 셋업하며, 제3감지점(DP43)에 선택된 루트에 장애가 검출되거나 제4감지점(DP44)에 선택된 루트가 기 사용중에 있는 상태로 검출되거나 제5감지점(DP45)에 선택된 루트를 통한 호 설정 셋업 메시지의 응답이 검출되지 않을 경우 예외 처리를 수행하는

다음 초기화 루틴으로 리턴되고, 선택된 루트를 통해 호 설정이 이루어지는 경우 호 처리점(PIC44)를 통해 발신호의 활성화 처리를 수행한다.

<44> 전술한 바와 같은 종래의 이동 통신망에서는 발신호 요구되는 단말기에 대하여 인증과 권한을 분석하여 적법한 단말기가 아닌 것으로 판단되거나 어떠한 이유로 인하여 인증에 실패하게 되는 경우 해당 단말기의 발신호에 대하여 무조건적으로 서비스를 차단하고 있으므로, 해당 가입자에 대한 신원 파악이나 해당 단말기에 대한 적법성 여부의 판단, 해당 단말기에 대한 적절한 조치를 수행할 수 없는 문제점이 있었다.

<45> 또한, 무조건적인 서비스의 차단으로 인하여 서비스 사용료를 납부하지 않은 가입자에 대하여 미납된 대금의 납부를 안내하고 정상적인 가입자로의 유도를 실행할 수 없는 문제점이 있었다.

【발명이 이루고자 하는 기술적 과제】

<46> 본 발명은 전술한 바와 같은 제반적인 문제점을 감안한 것으로, 그 목적은 통신 서비스 망에서, 가입자의 발신호가 어떠한 이유에 의하여 인증에 실패하거나 권한 부정된 경우 해당 가입자에 대한 서비스를 무조건적으로 차단하지 않고 고객센터 혹은 해당 단말기의 적법한 가입자가 지정한 전화번호로 통화를 연결하거나 IP(Intelligent Peripheral) 등 특별한 서비스 장치로 연결하거나 또는 정상적인 호 처리를 진행시켜 해당 가입자에 대한 신원 파악과 적법성 여부의 판단 및 상황에 적절한 다양한 음성 안내 혹은 정상적인 호 서비스의 제공, 해당 가입자와 고객센터 담당자와의 통화를 통해 정

상적인 서비스로 유도하도록 한 것이다.

<47> 또한, 본 발명은 인증에 실패하거나 권한이 부정된 가입자의 호에 대한 추적 및 이력 유지가 자동적으로 수행되도록 하며, 인증에 실패하거나 권한이 부정된 가입자에 대하여 통신 서비스 망 사업자가 그 밖에 매우 다양한 조치 및 서비스를 창출하여 상황에 적절하게 적용할 수 있도록 한 것이다.

【발명의 구성 및 작용】

<48> 상기한 바와 같은 목적을 달성하기 위한 본 발명은 지능망 서비스에서 호 발신을 시도한 가입자에 대한 인증이 실패하거나 권한이 부정되는 경우 해당 사실을 SCP에 통보하고, 상기 SCP에서 지시하는 바에 따라 해당 처리 동작을 수행시키는 발신호 권한 부정 감지점을 더 포함하는 것을 특징으로 한다.

<49> 또한, 본 발명은 가입자 단말기의 발신호가 이동 교환 시스템에 검출되면 해당 발신호 가입자에 대한 인증 및 권한 부여 분석을 수행하는 과정과, 상기 발신호 가입자에 대하여 권한이 부정되는 경우 해당 가입자 프로파일에 권한 실패 트리거가 활성화되어 있는지를 판단하는 과정과, 상기에서 권한 실패 트리거가 비활성화 상태이면 이동 교환 시스템에서 제공하는 안내 음성의 송출후 발신호를 해제하고, 활성화 상태이면 해당 트리거를 담당하는 SCP측에 가입자의 인증 실패 혹은 권한 부정 이유를 나타내는 파라메타와 가입자의 위치 정보를 포함하여 발신 요구 지시 메시지를 전송하는 과정과, 가입자의 발신 요구 지시 메시지의 분석에 따라 가입자의 발신호를 소정의 위치로 연결시키기 위한 발신 요구 반송 결과 메시지를 이동 교환 시스템측에 전송하는 과정 및, 발신 요구

반송 결과 메시지에 따라 가입자의 발신호를 해당하는 소정의 위치로 연결하여 호 설정하는 과정을 포함하는 것을 특징으로 한다.

<50> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 일 실시예를 상세히 설명하면 다음과 같다.

<51> 본 발명은 지능망 규격의 기본 호 상태 모델(BCSM)에 발신호에 대한 인증 실패나 권한 부정이 발생하는 경우에 대하여 인증 실패 및 권한 부정에 대한 사실을 SCP측에 통보하고, SCP로부터 지시하는 바에 따라 발신호에 대한 정보 수집과 정보 분석 처리 및 호 설정을 위한 루트의 선택을 수행하도록 하는 감지점을 더 포함하고, 발신호를 시도한 가입자에 대하여 인증이 실패하거나 권한이 부정되는 경우 그 상황을 SCP측에 통보하여 SCP에서의 지시에 따라 처리 루틴을 실행하도록 하는 권한 실패 트리거 유형 (Authorization_Failure Trigger Type)을 정의한다.

<52> 먼저, 도 5에서 알 수 있는 바와 같이, WIN 규격에서 정의한 기본 호 상태 모델에서 발신호에 대한 인증 및 권한 처리에서 해당 발신호에 대해 인증 실패 및 권한 부정이 발생하는 경우 이를 검출한 다음 SCP측에 보고하고, SCP에서의 지시에 따라 해당 발신호에 대한 정보 수집 처리와 정보 분석 처리 및 호 설정 루트 선택 처리 단계로 천이를 실행하는 감지점(DP100)을 더 포함하며, 감지점(DP100)에서의 신호 천이 루틴은 하기의 표 1과 같이 정의 된다.

<53>

【표 1】

From	To	Nature of BCSM Transition	비고
발신 호 권한 부정 DP	예외 처리 정보 수집 PIC 정보 분석 PIC 루트 선택 PIC	Basic Extended Extended Extended	신규정의
발신호 권한 처리 PIC	발신호 권한 확인 DP 발신 중단 DP 예외 처리 DP 발신호 권한 부정 DP	Basic Basic	기존규격 신규정의

<54> 상기와 같이 정의되는 신호 감지점(DP100)에서 연동되는 권한 실패 트리거 유형은 발신호 권한 부정 감지점에서 감지하여 트리거 되도록 하고, 트리거가 부여된 상태에서 기타의 조건이 충족될 때 트리거 동작되도록 하며, 가입자 별로 트리거가 부여되도록 하며, 이동 통신 가입자의 호 발신에 대하여 트리거가 적용되도록 하며, 서비스 교환 기능/호 제어기능이 발신호 권한 부정 감지점에서 유효한 트리거 조건을 감지하게 하는 기존 트리거의 유형을 권한 실패 트리거 유형으로 하며, SCP가 응답하지 못하는 경우의 장애 상황이 발생하면 해당 발신호를 종료하거나 해당 발신호를 미리 정한 곳으로 루팅하거나 혹은 정상적인 호 진행을 계속하도록 하며, 트리거 조건이 충족되었을 때는 TIA/EIA-41 상의 발신 요구 지시가 수행되도록 하며, 발신호 권한 부정 감지점을 만났음을 SCP로 통지하기 위한 조건을 등록 인식 결과 등에 의하여 수신하는 가입자 프로파일에 의하여 부여한다.

<55> 상기한 바와 같이 WIN 규격의 기본 호 상태 모델에 감지점(DP100)을 적용한 경우에 대하여 발신호 처리에 대한 동작은 다음과 같다.

- <56> 단말기의 발신호가 호 처리점(PIC1)에 검출되면 해당 호 처리점(PIC1)은 검출되는 발신호에 대하여 이벤트 처리를 수행한 다음 지능망 서비스를 위해 다음 단계로 천이시킨다.
- <57> 호 처리점(PIC2)은 발신호에 대하여 정상적인 가입자 단말기로부터의 발신호 인지의 여부를 판단하기 위해 단말기의 인증과 권한 여부를 검사하여 정상적인 가입자 단말기로부터의 발신호 인것으로 판단되어 인증과 권한이 부여되는 경우 전술한 바와같이 통상적인 처리 절차를 수행하므로 이에 대한 설명은 생략한다.
- <58> 만약, 상기 호 처리점(PIC2)에서 발신호 요구한 가입자 단말기에 대하여 인증 실패나 권한이 부정되면 이에 대한 정보가 감지점(DP100)에 검출되며, 감지점(DP100)은 인증 실패 또는 권한 부정된 가입자에 대한 정보를 상기한 바와 같이 정의되는 권한 실패 트리거 유형에 따라 SCP측에 보고한다.
- <59> 이후, 감지점(DP100)은 SCP로부터 지시되는 내용에 따라 인증 실패 또는 권한 부정된 발신호에 대하여 호 처리점(PIC3)을 통해 정보 수집 처리 루틴을 실행시키거나 호 처리점(PIC4)을 통해 정보 분석 처리 또는 호 처리점(PIC5)를 통해 호 설정을 위한 루트 선택 처리를 수행시켜 적법한 가입자가 지정한 전화번호로의 통화를 연결하거나 IP 등 특별한 서비스 장치로 호를 연결하거나 또는 정상적인 호 처리를 수행시켜 해당 가입자에 대한 신원 파악, 적법성 여부의 판단 및 상황에 적절한 음성 안내 서비스를 제공하여 준다.
- <60> 또한, 첨부된 도 6에서 알 수 있는 바와 같이 ITU-T 규격에서 정의한 기본 호 상태

모델에서 발신호에 대한 인증 및 권한 처리에서 해당 발신호에 대해 인증 실패 및 권한 부정이 발생하는 경우 이를 검출한 다음 SCP측에 보고하고, SCP에서의 지시에 따라 해당 발신호에 대한 정보 수집 처리 혹은 정보 분석 처리 및 호 설정을 위한 루트 선택 처리 단계로의 천이를 실행하는 감지점(DP200)을 더 포함하며, 감지점(DP200)에서의 신호 천이 루틴은 하기의 표 2와 같이 정의 된다.

<61> 【표 2】

From	To	Nature of BCSM Transition	비고
발신호 권한 부정 DP	예외 처리 정보 수집 PIC 정보 분석 PIC 루트 선택 PIC	Basic Extended Extended Extended	신규정의
발신호 권한 처리 PIC	발신호 권한 확인 DP 발신 중단 DP 예외 처리 DP 발신호 권한 부정 DP	Basic Basic	기존규격 신규정의

<62> 상기와 같이 정의되는 감지점(DP200)에서의 권한 실패 트리거 유형은 발신호 권한 부정 감지점에서 감지하여 트리거 되도록 하고, 트리거가 부여된 상태에서 기타의 조건이 충족될 때 트리거 동작되도록 하며, 가입자 별로 트리거가 부여되도록 하며, 이동 통신 가입자, 비 ISDN 유선 가입자, BRI 서비스 프로파일, BRI 정합, PRI 정합 등에 대하여 트리거가 적용되도록 하며, 서비스 교환 기능/호 제어기능이 발신호 권한 부정 감지점에서 유효한 트리거 조건을 감지하게 하는 기준 트리거의 유형을 권한 실패 트리거 유형으로 하며, SCP가 응답하지 못하는 경우의 장애 상황이 발생하면 해당 발신호를 종료하거나 해당 발신호를 미리 정한 곳으로 루팅하거나 혹은 정상적인 호 진행을 계속하도

록 정의한다.

- <63> 상기한 바와 같이 ITU-T 규격의 기본 호 상태 모델에 감지점(DP200)을 적용한 경우에 대하여 발신호 처리에 대한 동작은 다음과 같다.
- <64> 단말기의 발신호가 호 처리점(PIC21)에 검출되면 해당 호 처리점(PIC21)은 검출되는 발신호에 대하여 이벤트 처리를 수행한 다음 지능망 서비스를 위해 다음 단계로 천이시킨다.
- <65> 호 처리점(PIC22)은 발신호에 대하여 정상적인 가입자 단말기로부터의 발신호 인지의 여부를 판단하기 위해 단말기의 인증과 권한 여부를 검사하여 정상적인 가입자 단말기로부터의 발신호 인것으로 판단되어 인증과 권한이 부여되는 경우 전술한 바와같이 통상적인 처리 절차를 수행하므로 이에 대한 설명은 생략한다.
- <66> 만약, 상기 호 처리점(PIC22)에서 발신호 요구한 가입자 단말기에 대하여 인증 실패나 권한이 거부되면 이에 대한 정보가 감지점(DP200)에 검출되며, 감지점(DP200)은 발신호에 대한 가입자 정보를 상기한 바와 같이 정의 되는 트리거 유형에 따라 SCP측에 보고한다.
- <67> 이후, 감지점(DP200)은 SCP로부터 지시되는 내용에 따라 인증 실패 또는 권한 부정된 발신호에 대하여 호 처리점(PIC23)을 통해 정보 수집 처리 루틴을 실행시키거나 호 처리점(PIC24)을 통해 정보 분석 처리 또는 호 처리점(PIC25)을 통해 호 설정을 위한 루트 선택 처리를 수행시켜 적법한 가입자가 지정한 전화번호로의 통화를 연결하거나 IP 등 특별한 서비스 장치로 호를 연결하거나 또는 정상적인 호 처리를 수행시켜 해당 가입자에 대한 신원 파악, 적법성 여부의 판단 및 상황에 적절한 음성 안내 서비스를 제공하

여 준다.

<68> 또한, 첨부된 도 7에서 알 수 있는 바와 같이 CAMEL 규격에서 정의한 기본 호 상태 모델에서 발신호에 대한 인증 및 권한 처리에서 해당 발신호에 대해 인증 실패 및 권한 부정이 발생하는 경우 이를 검출한 다음 SCP측에 보고하고, SCP에서의 지시에 따라 해당 발신호에 대한 정보 분석 처리 혹은 호 설정을 위한 루트 선택 처리 단계로의 천이를 실행하는 감지점(DP300)을 더 포함하며, 감지점(DP300)에서의 신호 천이 루틴은 하기의 표 3과 같이 정의 된다.

<69> 【표 3】

From	To	Nature of BCSM Transition	비고
발신호 권한 부정 DP	예외 처리 정보 분석 PIC 루트 설정 및 착신응답대기	Basic Extended Extended	신규정의
발신호 권한 및 정보 수집 PIC	정보 수집 DP 발신호 권한 부정 DP	Basic Basic	기존규격 신규정의

<70> 상기한 바와 같이 정의되는 신호 감지점(DP300)에서의 권한 실패 트리거 유형은 발신호 권한 부정 감지점에서 감지하여 트리거 되도록 하고, 트리거가 부여된 상태에서 기타의 조건이 충족될 때 트리거 동작되도록 하며, 가입자 별로 트리거가 부여되도록 하며, 이동 통신 가입자의 호 발신에 대하여 트리거가 적용되도록 하며, 서비스 교환 기능/호 제어기능이 발신호 권한 부정 감지점에서 유효한 트리거 조건을 감지하게 하는 기준 트리거의 유형을 권한 실패 트리거 유형으로 하며, SCP가 응답하지 못하는 경우의 장애 상황이 발생하면 해당 발신호를 종료하거나 해당 발신호를 미리 정한 곳으로 루팅하

거나 혹은 정상적인 호 진행을 계속하도록 정의한다.

<71> 상기한 바와 같이 CAMEL 규격의 기본 호 상태 모델에 감지점(DP300)을 적용한 경우에 대하여 발신호 처리에 대한 동작은 다음과 같다.

<72> 발신호에 대한 이벤트가 호 처리점(PIC41)에 검출됨에 따라 해당 호 처리점(PIC41)에서는 발신호에 대한 인증 및 권한 부여 여부를 분석하고, 발신호에 대한 초기 정보의 수집을 수행한다.

<73> 이때, 해당 발신호의 인증 및 권한 부여 분석에서 해당 발신호에 대하여 인증 및 권한 부여가 정상적으로 이루어지는 경우 수집된 정보의 분석 의뢰와 발신호의 루팅 및 감시, 발신호의 활성화 처리 등의 통상적인 동작을 실행하므로, 이에 대한 동작 관계는 생략한다.

<74> 만약 해당 발신호에 대한 인증 및 권한 부여 분석에서 발신호에 대하여 인증에 실패하거나 권한 부여가 거부되면 그에 대한 정보가 감지점(DP300)에 검출된다.

<75> 따라서, 감지점(DP300)은 상기한 바와 같이 정의되는 트리거 유형에 따라 해당 발신호 가입자에 대한 정보를 SCP측에 보고하고, SCP에서 지시되는 정보에 따라 호 처리점(PIC42)을 통해 발신호에 대한 정보 분석을 수행시키거나 호 처리점(PIC43)을 통해 발신호에 대하여 호 설정을 위한 루팅 및 착신 응답 대기를 수행시켜 적법한 가입자가 지정한 전화번호로의 통화를 연결하거나 IP 등 특별한 서비스 장치로 호를 연결하거나 또는 정상적인 호 처리를 수행시켜 해당 가입자에 대한 신원 파악, 적법성 여부의 판단 및 상황에 적절한 음성 안내 서비스를 제공하여 준다.

- <76> 본 발명에 따라 인증 실패 및 권한 부정 검출시 적절한 호 설정 서비스의 절차에 대하여 설명하면 다음과 같다.
- <77> 먼저, 일예를 들어 WIN 규정에서의 발신호에 대한 서비스 절차에 대하여 첨부된 도 8을 참조하여 설명하면 다음과 같다.
- <78> 이동 통신 서비스 망에서 임의의 단말기(10)로부터의 발신호가 이동 교환 시스템인 MSC/VLR(20)에 감지되면(S501) MSC/VLR(20)은 감지되는 발신호에 대하여 인증 절차를 수행하는데, MSC/VLR(20)은 해당 발신호에 대하여 필요에 따라 도시되지 않은 HLR이나 인증센터로 인증 요구 메시지를 이용하여 인증절차를 수행하며, 발신호 요구한 단말기(10)에 대한 인증이 실패하거나 어떤 이유에 의하여 발신 가입자에 대한 권한이 부정되면 발신호 권한 부정 감지점으로 천이한다(S503).
- <79> 상기 발신호 권한 부정 감지점에서 발신호 가입자에 대한 프로파일(Profile)에 권한 실패 트리거(Authorization_Failure Trigger)가 활성화 되어 있지 않으면 MSC/VLR(20)은 발신호 요구한 단말기(10)측에 자체적으로 제공되는 적절한 안내 방송을 송출한 다음 호 해제 및 모든 자원을 해제한다(S504).
- <80> 그러나, 상기 권한 부정 감지점에서 발신호 가입자의 프로파일에 권한 실패 트리거가 활성화되어 있는 상태이면 해당 트리거를 담당하는 SCP(30)측에 가입자에 대한 인증 실패 혹은 권한 부정의 이유를 나타내는 파라메타와 가입자의 현재 위치 정보가 포함되는 발신 요구 지시(OriginationRequest INVOKE) 메시지를 전송한다(S505).
- <81> 이때, SCP(30)은 수신되는 발신 요구 지시 메시지에서 발신호 요구한 가입자 단말기(10)의 인증 실패 혹은 권한 부정의 이유와 해당 단말기(10)의 위치 정보를 가입자의

프로파일과 인증 실패 및 권한 부정 이력을 참조하여 분석한 후 필요한 사항을 저장하고, 다음 루틴을 선택하여 수행한다.

<82> 먼저, SCP(30)는 해당 가입자 단말기(10)의 발신호에 대하여 고객 서비스 센터의 해당 인증실패 혹은 권한 부정 사항을 담당하는 그룹으로 연결하거나 해당 단말기(10)의 적법한 가입자가 지정한 전화번호로 연결하여야 한다고 판단되면 발신요구 반송 결과(OriginationRequest RETURN RESULT) 메시지에 해당 인증 실패 혹은 권한 부정 사항을 담당하는 고객센터내 그룹으로의 루팅 번호나 해당 단말기(10)의 적법한 가입자가 지정한 전화번호를 포함시키고, 선택적으로는 발신 가입자의 번호(Calling Party Number)를 착신자에게 제공하도록 하는 내용을 포함시켜 MSC/VLR(20)측에 전송하며, 상기 SCP(30)가 발신호 요구한 가입자 단말기(10)에 대하여 IP(50)로 호를 연결하여 특별한 목적의 음성 안내 방송을 듣게 하여야 한다고 판단되는 경우 그 특별한 음성 안내 방송을 송출하는 IP(50)로의 루팅 번호가 알려져 있으면 해당 루팅번호를 발신 요구 반송 결과(OriginationRequest RETURN RESULT) 메시지에 포함시켜 MSC/VLR(20)측에 전송한다(S508).

<83> 만약, 상기에서 SCP(30)가 발신호 요구한 가입자 단말기(10)에 대하여 IP(50)로 호를 연결하여 특별한 목적의 음성 안내 방송을 듣게 하여야 한다고 판단되는 경우 그 특별한 음성 안내 방송을 송출하는 IP(50)로의 루팅 번호가 알려져 있지 않은 상태이면 SCP(30)는 발신호 요구한 해당 가입자에게 특별한 목적의 음성 안내 방송을 제공할 IP(50)로 자원 점유 지시(SeizeResoure INVOKE)를 요구한 다음(S506), IP(50)로부터 안내방송을 액세스 할 수 있도록 TLDN(Temporary Local Directory Number)이 실려있는 자원 점유 반송 결과(OriginationRequest RETURN RESULT) 메시지를 수신한 다음(S507)

TLDN을 발신 요구 반송 결과 정보를 포함시켜 MSC/VLR(20)측에 전송한다(S508).

<84> 만약, 상기에서 SCP(30)가 그 가입자에 대하여 정상적인 호 발신 처리를 계속해 주어야 한다고 판단하면 정상적인 호 진행을 계속할 것을 지시하는 파라미터를 실어 발신 요구 반송 결과 메시지를 MSC/VLR(20)측에 전송한다(S508).

<85> 이때, MSC내부에서 제공하는 특정 안내방송을 송출할 것을 지시하는 파라미터를 포함할 수 도 있다.

<86> 또한, 상기에서 SCP(30)가 발신호에 대한 호 처리를 중단하고 모든 자원의 회수가 필요하다고 판단되면 발신 요구 반송 결과(OriginationRequest RETURN RESULT) 메시지에 호 처리 중단을 지시하는 내용을 포함시켜 상기 MSC/VLR(20)측에 전송한다(S508).

<87> 따라서, 상기 MSC/VLR(20)은 상기한 바와 같이 SCP(30)로부터 수신되는 발신 요구 반송 결과에 따라 인증 실패 혹은 권한 부정된 발신호에 대하여 적절한 연결을 수행한다

<88> 상기에서 SCP(30)에서 수신되는 발신 요구 반송 결과가 특정한 루팅번호나 혹은 착신번호로 연결하여 설정할 것을 지시하는 경우 그것이 고객센터의 특정 그룹이나 혹은 해당 단말기(10)의 적법한 가입자가 미리 지정한 전화번호로의 호 설정을 지시하는 것이면 MSC/VLR(20)은 발신호 단말기(10)와 고객센터 혹은 미리 지정된 가입자(40)를 연결하여 주고(S509), IP(50)로의 호 설정을 지시하는 것이면 MSC/VLR(20)은 발신호 단말기(10)와 IP(50)간의 호를 설정하여 주며(S510), 정상적인 발신호 처리를 수행할 것을 지시하는 경우 MSC/VLR(20)은 발신호와 피 호출자(60)를 연결하여 주며(S511), 해당 발신호에 대한 호 처리 중단 지시이면 MSC/VLR(20)은 해당 발신호에 대하여 호 해제를 수행

한다(S512).

<89> 상기 S509에서 MSC/VLR(20)이 고객센터의 해당 인증실패 혹은 권한 부정 사항을 담당하는 고객센터의 그룹으로 호를 설정하게 되면 고객센터에서는 담당하는 문제에 따라 발신호 가입자에 대한 신원 파악과 적법성 여부의 판단을 수행하고, 불법으로 복제하여 사용하는 가입자에 대해서는 단말기의 회수 유도 및 정상적인 서비스로의 인도, 혹은 해당 가입자에 대한 서비스 배제 여부 판단 등을 수행하며, 해당 내용을 기록 유지하고 필요시 서비스 프로파일에 반영한다.

<90> 그리고, 가입자가 서비스 사용료를 지불하고 있는 경우 해당하는 사항을 가입자에게 음성 안내를 통해 통보하여 정상적인 서비스로 유도하며, 가입자가 적법한 경우임에도 인증에 실패하거나 권한이 부정되는 경우에는 해당 가입자에 대한 서비스가 조기에 정상화 될 수 있는 조치를 취해 주거나 필요한 안내 서비스를 제공하여 준다.

<91> 그리고, MSC/VLR(20)에서 발신호에 대하여 적법한 가입자가 미리 지정한 전화번호로 호를 설정하게 되면 미리 지정된 착신측에서 발신자에 대한 신원을 확인하고 단말기가 회수 될 수 있도록 유도하여 준다.

<92> 상기 S510에서 MSC/VLR(20)에 IP(50)로 호를 연결하게 되면 IP(50)는 해당 착신 루팅번호에 해당하는 특별한 음성 안내 방송을 가입자에게 송출하며, 안내 방송의 송출이 완료되면 설정된 호를 종료한다.

<93> 상기 S511에서는 MSC/VLR(20)이 인증 실패 혹은 권한 부정된 발신호에 대하여 발신 가입자가 호출한 번호로 호를 설정하고 정상적인 서비스를 제공한다.

<94> 이때, SCP(30)가 MSC/VLR(20)내부에서 제공하는 특정 안내방송을 송출할 것을 지시

하였으면 해당 안내 방송이 발신자에게 제공되며, 피 호출자와의 통화가 종료되면 설정된 호를 해제한다.

<95> 또한, 상기 S505에서 MSC/VLR(20)로부터 가입자에 대한 인증 실패 혹은 권한 부정의 이유를 나타내는 파라메타와 가입자의 현재 위치 정보가 포함된 발신 요구 지시 (OriginationRequest INVOKE) 메시지를 SCP(30)가 수신하는 경우 SCP(30)가 그 가입자에 대하여 IP(50)등 서비스 장치로 호를 연결하여 가입자와 그 서비스 장치간에 상호 동작을 취하면서 특별한 목적의 서비스를 수행할 필요가 있다고 판단하면 SCP(30)는 특별한 목적의 서비스를 수행할 수 있는 자원 점유 지시를 IP(50)측에 요구하고(S513), IP(50)는 SCP(30)로부터의 자원 점유 지시 요구에 따라 지정된 자원을 액세스 할 수 있는 TLDN을 실어 자원 점유 반송 결과 메시지를 SCP(30)측에 전송한다(S514).

<96> 이때, SCP(30)는 자원 점유 반송 결과 메시지에 포함된 TLDN을 포함하여 MSC/VLR(20)측에 자원 연결을 지시하는 메시지를 전송하게 되면(S515) MSC/VLR(20)은 TLDN을 이용하여 발신호의 단말기(10)를 IP(50)와 호를 설정한다(S516).

<97> 상기와 같이 발신호 단말기(10)와 IP(50)간의 호 설정이 이루어지면 IP(50)는 특별한 목적의 서비스를 수행할 자원에 대하여 할당한 TLDN으로 호가 접속되었음을 감지하고 그에 대한 사실을 SCP(30)측에 통보하며, 해당 호에 대해서 어떠한 처리를 수행할 것 인지를 요청하기 위한 명령 요구 지시 메시지를 SCP(30)측에 전송한다(S517).

<98> 이때, SCP(30)는 상기 명령 요구 지시 메시지에 따라 지정된 자원에 대한 동작을 지시하는 내용에 대한 특수 자원 기능 명령 지시 메시지를 IP(50)측에 전송하면(S518) IP(50)는 지정된 자원에 대하여 특수자원 기능 명령 지시 메시지가 지시하는 동작을 발신호 가입자와 상호 동작을 취하면 수행한다(S519).

- <99> 상기와 같이 발신호 가입자와 IP(50)간의 상호 작용이 종료되면 IP(50)는 그 결과에 따라서 정보를 실시 자원기능 명령 반송 결과 메시지를 SCP(30)측에 통보하고(S520), SCP(30)는 발신 요구 반송 결과 메시지에 상기 특수자원기능 명령 반송 결과의 내용을 포함시켜 MSC/VLR(20)측에 전송하며(S521), 명령 요구 반송 결과를 IP(50)측에 전송한다(S522).
- <100> 이때, MSC/VLR(20)은 SCP(30)로부터 수신되는 발신 요구 반송 결과 메시지의 지시에 따라 새로운 호를 설정하거나 호 해제를 수행한다(S523)(S524).
- <101> 또한, 다른 일예로 ITU-T 규정에서의 발신호에 대한 서비스 절차에 대하여 첨부된 도 9를 참조하여 설명하면 다음과 같다.
- <102> 임의의 단말기(10)로부터의 발신호가 교환기/SSP(20A)에 감지되면(S601) 교환기/SSP(20A)는 감지되는 발신호에 대하여 인증 절차를 수행하며(S602), 발신호 요구한 단말기(10)에 대한 인증이 실패하거나 어떤 이유에 의하여 발신 가입자에 대한 권한이 부정되면 발신호 권한 부정 감지점으로 천이한다(S603).
- <103> 상기 발신호 권한 부정 감지점에서 발신호 가입자에 대한 프로파일에 권한 실패 트리거가 활성화 되어 있지 않으면 교환기/SSP(20A)는 발신호 요구한 단말기(10)측에 자체적으로 제공되는 적절한 안내 방송을 송출한 다음 호 해제 및 모든 자원을 해제한다(S604).
- <104> 그러나, 상기 권한 부정 감지점에 발신호 가입자의 프로파일에 권한 실패 트리거가 활성화되어 있는 상태이면 해당 트리거를 담당하는 SCP(30)측에 가입자에 대한 인증 실

패 혹은 권한 부정의 이유를 나타내는 파라메타와 가입자의 현재 위치 정보를 포함하여 초기 감지점(InitialDP) 메시지를 전송한다(S605).

<105> 이때, SCP(30)는 수신되는 초기 감지점 메시지로부터 발신호 가입자의 인증 실패 혹은 권한 부정의 이유와 위치 정보를 가입자 프로파일과 인증 실패 및 권한 부정 이력을 참조하여 분석한 후 필요한 사항을 저장하고, 다음의 각 처리 과정을 선택하여 수행한다.

<106> 만약, 상기 SCP(30)가 가입자의 발신호를 고객 센터의 해당 인증 실패 혹은 권한 부정 사항을 담당하는 그룹으로 연결하거나 해당 단말기의 적법한 가입자가 지정한 전화번호로 연결하여야 된다고 판단되는 경우 SCP(30)는 해당 인증 실패 혹은 권한 부정 사항을 담당하는 고객센터내 그룹으로의 루팅번호나 해당 단말기의 적법한 가입자가 지정한 전화번호를 포함하는 연결(Connect) 메시지를 교환기/SSP(20A)측에 전송하여 주고, 가입자의 발신호에 대하여 IP(50)로 호를 연결하여 특별한 목적의 음성 안내방송을 듣게 하여야 한다고 판단되는 경우 그 특별한 음성 안내 방송을 송출하는 IP(50)로의 루팅번호를 연결 메시지에 포함시켜 교환기/SSP(20A)측에 전송한다(S606).

<107> 이때, 교환기/SSP(20A)는 상기 SCP(30)로부터의 연결 메시지의 지시에 따라 해당하는 동작을 수행하는데, 만약 가입자의 호를 특정한 루팅번호 혹은 착신번호로의 연결 설정을 지시하는 경우 그것이 고객센터의 특정 그룹이나 혹은 해당 단말기의 적법한 가입자가 미리 지정한 전화번호로의 호 설정을 지시하는 것이면 발신호 가입자와 고객센터 혹은 미리 지정된 착신자(40)와 호 설정을 수행하고(S607), IP(50)로의 호 설정을 지시하는 것이면 발신호 가입자와 IP(50)간의 호를 설정하여 준다(S608).

<108> 만약, SCP(30)가 가입자 발신호에 대하여 정상적인 호 발신 처리를 유지하여

주어야 한다고 판단되어 계속 메시지를 교환기/SSP(20A)측에 전송하면 발신호 가입자가 호출한 번호의 피호출자(60)를 호출하여 발신호 가입자와 피호출자(60)간의 호를 설정하여 통화를 유지하여 준다(S609)(S610).

<109> 만약, SCP(30)가 발신호에 대한 호처리를 중단하고 모든 자원의 회수가 필요하다고 판단하면 호 해제 메시지를 교환기/SSP(20A)측에 전송한다(S611).

<110> 상기와 같이 교환기/SSP(20A)에서 고객센터의 해당 인증실패 혹은 권한 부정 사항을 담당하는 고객센터의 그룹으로 호를 설정하게 되면 고객센터에서는 담당하는 문제에 따라 발신호 가입자에 대한 신원 파악과 적법성 여부의 판단을 수행하고, 불법으로 복제하여 사용하는 가입자에 대해서는 단말기의 회수 유도 및 정상적인 서비스로의 인도, 혹은 해당 가입자에 대한 서비스 배제 여부 판단 등을 수행하며, 해당 내용을 기록 유지하고 필요시 서비스 프로파일에 반영한다.

<111> 그리고, 가입자가 서비스 사용료를 체불하고 있는 경우 해당하는 사항을 가입자에게 음성 안내를 통해 통보하여 정상적인 서비스로 유도하며, 가입자가 적법한 경우임에도 인증에 실패하거나 권한이 부정되는 경우에는 해당 가입자에 대한 서비스가 조기에 정상화 될 수 있는 조치를 취해 주거나 필요한 안내 서비스를 제공하여 준다.

<112> 그리고, 발신호에 대하여 적법한 가입자가 미리 지정한 전화번호로 호를 설정하게 되면 미리 지정된 착신측에서 발신자에 대한 신원을 확인하고 단말기가 회수 될 수 있도록 유도하여 준다.

<113> 또한, SCP(30)가 IP(50)의 자원을 이용하여 발신호 가입자에게 특별한 목적의 서비스를 수행하기 위하여 해당 특별한 목적의 IP자원으로의 주소 정보를 실어 교환기

/SSP(20A)에 자원 연결 메시지를 전송하고(S613), 동시에 IP(50)측에 안내 방송 송출을 요구하는 메시지를 전송하면(S614) 교환기/SSP(20A)는 자원 연결 메시지에서 SCP(30)가 지정하는 IP(50)의 주소로 호를 설정하며, IP와 발신호 가입자간의 상호 동작에 의해 특별한 목적의 서비스 절차가 수행된다(S615).

<114> 또한, 다른 일 예를 CAMEL 규정에서의 발신호에 대한 서비스 절차에 대하여 첨부된 도 10를 참조하여 설명하면 다음과 같다.

<115> 임의의 단말기(10)로부터의 발신호가 MSC/VLR/gsmSSF(20C)에 감지되면(S701) MSC/VLR/gsmSSF(20C)는 감지되는 발신호에 대하여 인증 절차를 수행하며(S702), 발신호 요구한 단말기(10)에 대한 인증이 실패하거나 어떤 이유에 의하여 발신 가입자에 대한 권한이 부정되면 발신호 권한 부정 감지점으로 천이한다(S703).

<116> 상기 발신호 권한 부정 감지점에서 발신호 가입자에 대한 프로파일에 권한 실패 트리거가 활성화 되어 있지 않으면 MSC/VLR/gsmSSF(20C)는 발신호 요구한 단말기(10)측에 자체적으로 제공되는 적절한 안내 방송을 송출한 다음 호 해제 및 모든 자원을 해제한다(S704).

<117> 그러나, 상기 권한 부정 감지점에 발신호 가입자의 프로파일에 권한 실패 트리거가 활성화되어 있는 상태이면 해당 트리거를 담당하는 SCP(30)측에 가입자에 대한 인증 실패 혹은 권한 부정의 이유를 나타내는 파라메타와 가입자의 현재 위치 정보를 포함하여 초기 감지점(InitialDP) 메시지를 전송한다(S705).

<118> 이때, SCP(30)는 수신되는 초기 감지점 메시지에서 발신호 가입자의 인증 실패

혹은 권한 부정의 이유와 위치 정보, 가입자 프로파일과 인증 실패 및 권한 부정 이력을 참조하여 분석한 후 필요한 사항을 저장하고, 다음의 각 처리 과정을 선택하여 수행한다.

<119> 만약, 상기 SCP(30)가 가입자의 발신호를 고객 센터의 해당 인증 실패 혹은 권한 부정 사항을 담당하는 그룹으로 연결하거나 해당 단말기의 적법한 가입자가 지정한 전화번호로 연결하여야 된다고 판단되는 경우 SCP(30)는 해당 인증 실패 혹은 권한 부정 사항을 담당하는 고객센터내 그룹으로의 루팅번호나 해당 단말기의 적법한 가입자가 지정한 전화번호를 포함하는 연결(Connect) 메시지를 MSC/VLR/gsmSSF(20C)측에 전송하여 주고, 가입자의 발신호에 대하여 IP(50)로 호를 연결하여 특별한 목적의 음성 안내방송을 듣게 하여야 한다고 판단되는 경우 그 특별한 음성 안내 방송을 송출하는 IP(50)로의 루팅번호를 연결 메시지에 포함시켜 MSC/VLR/gsmSSF(20C)측에 전송한다(S706).

<120> 이때, MSC/VLR/gsmSSF(20C)는 상기 SCP(30)로부터의 연결 메시지의 지시에 따라 해당하는 동작을 수행하는데, 만약 가입자의 호를 특정한 루팅번호 혹은 착신번호로의 연결 설정을 지시하는 경우 그것이 고객센터의 특정 그룹이나 혹은 해당 단말기의 적법한 가입자가 미리 지정한 전화번호로의 호 설정을 지시하는 것이면 발신호 가입자와 고객센터 혹은 미리 지정된 착신자(40)와 호 설정을 수행하고(S707), IP(50)로의 호 설정을 지시하는 것이면 발신호 가입자와 IP(50)간의 호를 설정하여 준다(S708).

<121> 만약, SCP(30)가 가입자 발신호에 대하여 정상적인 호 발신 처리를 유지하여 주어야 한다고 판단되어 계속 메시지를 MSC/VLR/gsmSSF(20C)측에 전송하면 발신호 가입자가 호출한 번호의 피호출자(60)를 호출하여 발신호 가입자와 피호출자(60)간의 호를 설정하여 통화를 유지하여 준다(S709)(S710).

- <122> 만약, SCP(30)가 발신호에 대한 호 처리를 중단하고 모든 자원의 회수가 필요하다 고 판단하면 호 해제 메시지를 MSC/VLR/gsm SSF(20C)측에 전송한다(S711).
- <123> 상기와 같이 MSC/VLR/gsmSSF(20C)에서 고객센터의 해당 인증실패 혹은 권한 부정 사항을 담당하는 고객 센터의 그룹으로 호를 설정하게 되면 고객 센터에서는 담당하는 문제에 따라 발신호 가입자에 대한 신원 파악과 적법성 여부의 판단을 수행하고, 불법으로 복제하여 사용하는 가입자에 대해서는 단말기의 회수 유도 및 정상적인 서비스로의 인도, 혹은 해당 가입자에 대한 서비스 배제 여부 판단 등을 수행하며, 해당 내용을 기록 유지하고 필요시 서비스 프로파일에 반영한다.
- <124> 그리고, 가입자가 서비스 사용료를 체불하고 있는 경우 해당하는 사항을 가입자에게 음성 안내를 통해 통보하여 정상적인 서비스로 유도하며, 가입자가 적법한 경우임에도 인증에 실패하거나 권한이 부정되는 경우에는 해당 가입자에 대한 서비스가 조기에 정상화 될 수 있는 조치를 취해 주거나 필요한 안내 서비스를 제공하여 준다.
- <125> 그리고, 발신호에 대하여 적법한 가입자가 미리 지정한 전화번호로 호를 설정하게 되면 미리 지정된 착신측에서 발신자에 대한 신원을 확인하고 단말기가 회수 될 수 있도록 유도하여 준다.
- <126> 또한, SCP(30)가 IP(50)의 자원을 이용하여 발신호 가입자에게 특별한 목적의 서비스를 수행하기 위하여 해당 특별한 목적의 IP자원으로의 주소 정보를 실어 MSC/VLR/gsmSSF(20C)에 자원 연결 메시지를 전송하고(S713), 동시에 IP(50)측에 안내 방송 송출을 요구하는 메시지를 전송하면(S714) MSC/VLR/gsmSSF(20C)는 자원 연결 메시지 에서 SCP(30)가 지정하는 IP(50)의 주소로 호를 설정하며, IP와 발신호 가입자간의 상호

동작에 의해 특별한 목적의 서비스 절차가 수행된다(S715).

【발명의 효과】

- <127> 이상에서 설명한 바와 같이 본 발명은 통신 서비스 망에서 가입자 발신호에 대하여 인증 실패 혹은 권한 부정된 경우 효과적인 조치 및 서비스를 다양하게 제공하며, 불법으로 복제하여 사용하는 단말기를 검출하여 적법한 가입자의 선의적인 피해를 방지하여 주며, 분실되거나 도난된 단말기를 원래의 주인에게 회수하여 주도록 한다.
- <128> 또한, 권한 부정된 가입자에 대한 효과적인 안내 음성 서비스를 제공하여 주며, 서비스 사용료를 체불한 가입자에 대하여 체불 상황을 고객센터의 안내를 통해 통보하여 정상적인 서비스로 유도하여 주며, 적법한 가입자의 단말기가 어떠한 이유에 의하여 인증에 실패하여 정상적인 서비스를 제공받지 못하는 경우 그 상황을 신속하게 파악하여 적절한 조치를 취해줌으로써 정상적인 서비스가 이루어지도록 한다.
- <129> 또한, 인증에 실패하거나 권한 부정된 가입자의 호에 대한 추적 및 이력 유지가 자동으로 가능하도록 하고, 인증 실패 및 권한 부정된 가입자의 호에 대하여 통신망 사업자가 매우 다양한 방법을 창출하여, 상황에 따라 적절하게 적용할 수 있도록 한다.

【특허청구범위】**【청구항 1】**

호 발신을 시도한 가입자에 대한 인증이 실패하거나 권한이 부정되는 경우 해당 사실을 SCP에 통보하고, 상기 SCP에서 지시하는 바에 따라 해당 처리 동작을 수행시키는 발신호 권한 부정 감지점을 더 포함하는 것을 특징으로 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법.

【청구항 2】

청구항 1에 있어서,

상기 발신호 권한 부정 감지점은 상기 SCP에서 지시하는 바에 따라 권한 부정된 발신호에 대한 정보 수집 처리와 수집된 정보의 분석 처리 및 분석된 발신호의 정보에 따라 호 설정을 위한 루트의 선택 처리를 실행시키는 것을 특징으로 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법.

【청구항 3】

청구항 1에 있어서,

상기 발신호 권한 부정 감지점은 검출되는 발신호 가입자의 프로파일이 활성화되어 있지 않은 상태이면 예외 처리를 수행하는 것을 특징으로 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법.

【청구항 4】

청구항 1에 있어서,

상기 발신호 권한 부정 감지점은 호 발신을 시도한 가입자의 인증 실패 혹은 권한 부정이 검출되는 경우 해당 사실을 SCP측에 통지하여 주는 권한 실패 트리거 유형이 정의 되는 것을 특징으로 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법.

【청구항 5】

가입자 단말기의 발신호가 이동 교환 시스템에 검출되면 해당 발신호 가입자에 대한 인증 및 권한 부여 분석을 수행하는 과정과;

상기 발신호 가입에 대하여 권한이 부정되는 경우 해당 가입자 프로파일에 권한 실패 트리거가 활성화되어 있는지를 판단하는 과정과;

상기에서 권한 실패 트리거가 비활성화 상태이면 교환 시스템에서 제공하는 안내 음성의 송출후 발신호를 해제하고, 활성화 상태이면 해당 트리거를 담당하는 SCP측에 가입자의 인증 실패 혹은 권한 부정 이유를 나타내는 파라메타와 가입자의 위치 정보를 포함하여 발신 요구 지시 메시지를 전송하는 과정과;

가입자의 발신 요구 지시 메시지의 분석에 따라 가입자의 발신호를 소정의 위치로 연결시키기 위한 발신 요구 반송 결과 메시지를 교환 시스템측에 전송하는 과정 및;

발신 요구 반송 결과 메시지에 따라 가입자의 발신호를 해당하는 소정의 위치로 연결하여 호 설정하는 과정을 포함하는 것을 특징으로 하는 인증 실패/권한 부정 가입자에

대한 지능망적 처리방법.

【청구항 6】

청구항 5에 있어서,

상기 SCP에서 수신되는 발신 요구 반송 결과 메시지에 인증 실패 혹은 권한 부정 사항을 담당하는 고객센터내 그룹으로의 루팅 번호나 해당 단말기의 적법한 가입자가 지정한 전화번호 정보가 포함되어 있는 경우 가입자의 발신호를 고객센터 혹은 지정된 착신자와 호 설정하여 주는 것을 특징으로 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법.

【청구항 7】

청구항 5에 있어서,

상기 SCP에서 수신되는 발신 요구 반송 결과 메시지에 특별한 목적의 안내 방송 송출을 위한 정보가 포함되어 있는 경우 루팅 번호에 지정되어 있는 IP와 가입자의 발신호를 연결하여 호 설정하는 것을 특징으로 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법.

【청구항 8】

청구항 5에 있어서,

상기 SCP에서 수신되는 발신 요구 반송 결과 메시지에 해당 가입자에 대하여 정상

적인 호 처리 수행을 지시하는 정보가 포함되는 경우 가입자가 호출하는 번호의 피호출자와 호 설정하는 것을 특징으로 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법.

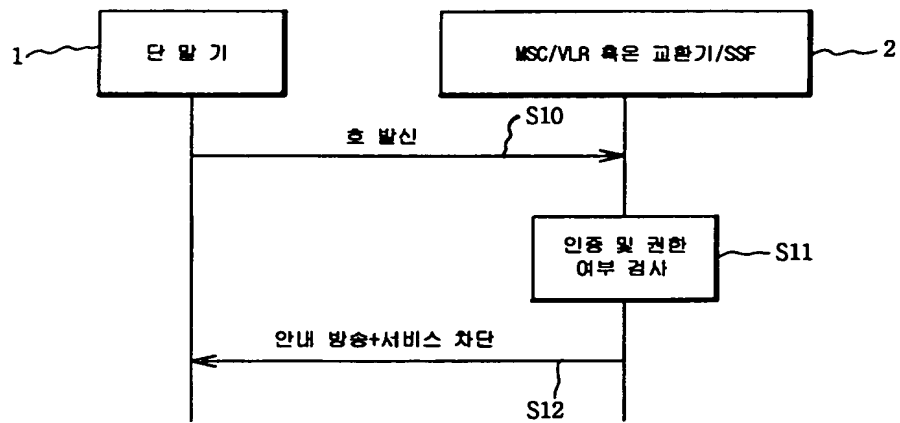
【청구항 9】

청구항 5에 있어서,

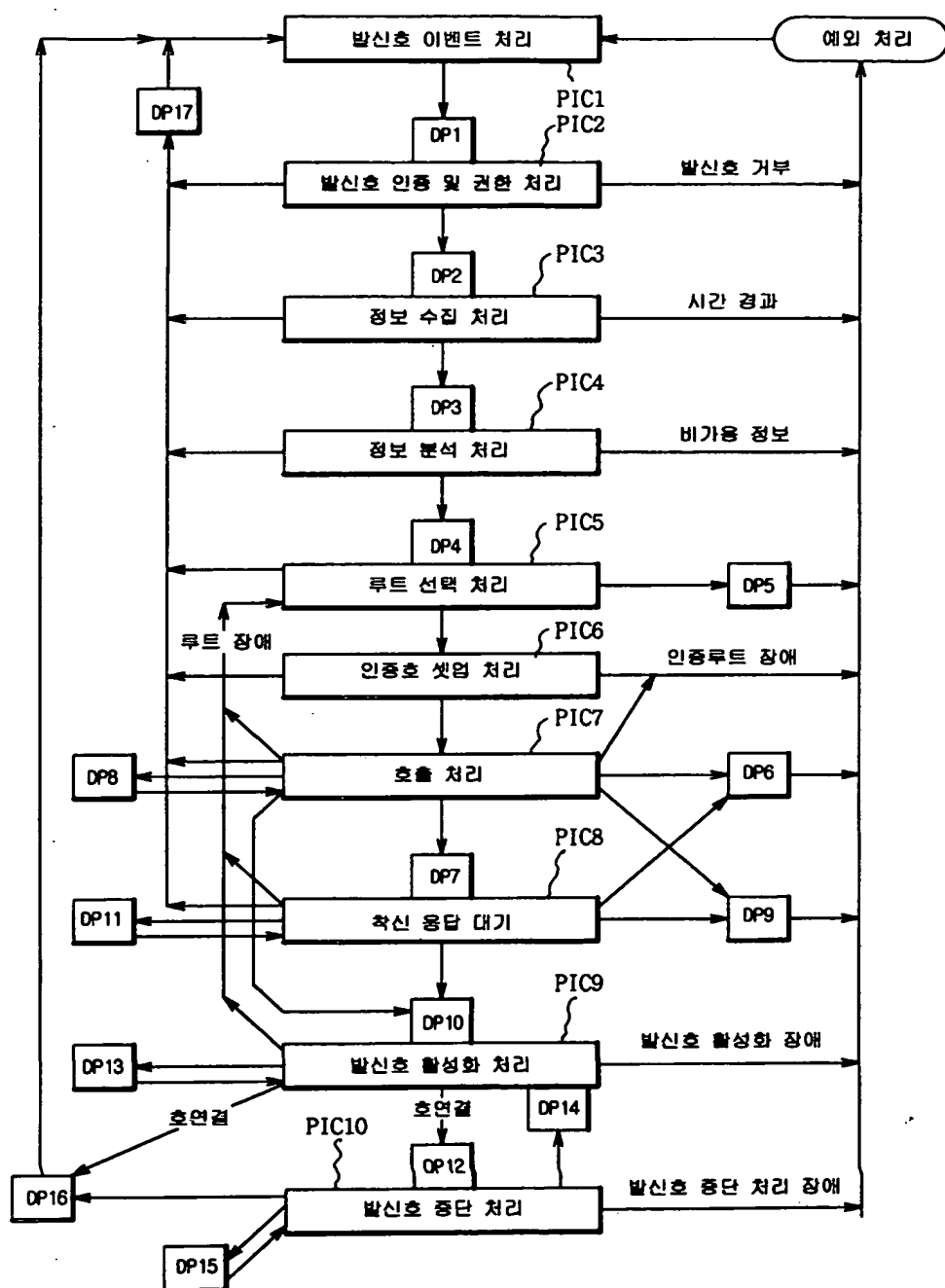
상기 발신 요구 지시 메시지를 수신한 SCP에 특정 안내 방송 및 특별한 목적의 서비스를 제공하는 IP의 루팅 번호가 지정되어 있지 않은 경우 해당 가입자에게 제공하고 자 하는 안내 방송 및 특별한 목적의 서비스 정보 파라메타를 포함하여 해당 IP측에 자원 점유 지시하고, 해당 IP로 부터 해당 안내 방송 및 특별한 목적의 서비스를 액세스 할 수 있는 자원을 할당 받는 것을 특징으로 하는 인증 실패/권한 부정 가입자에 대한 지능망적 처리방법.

【도면】

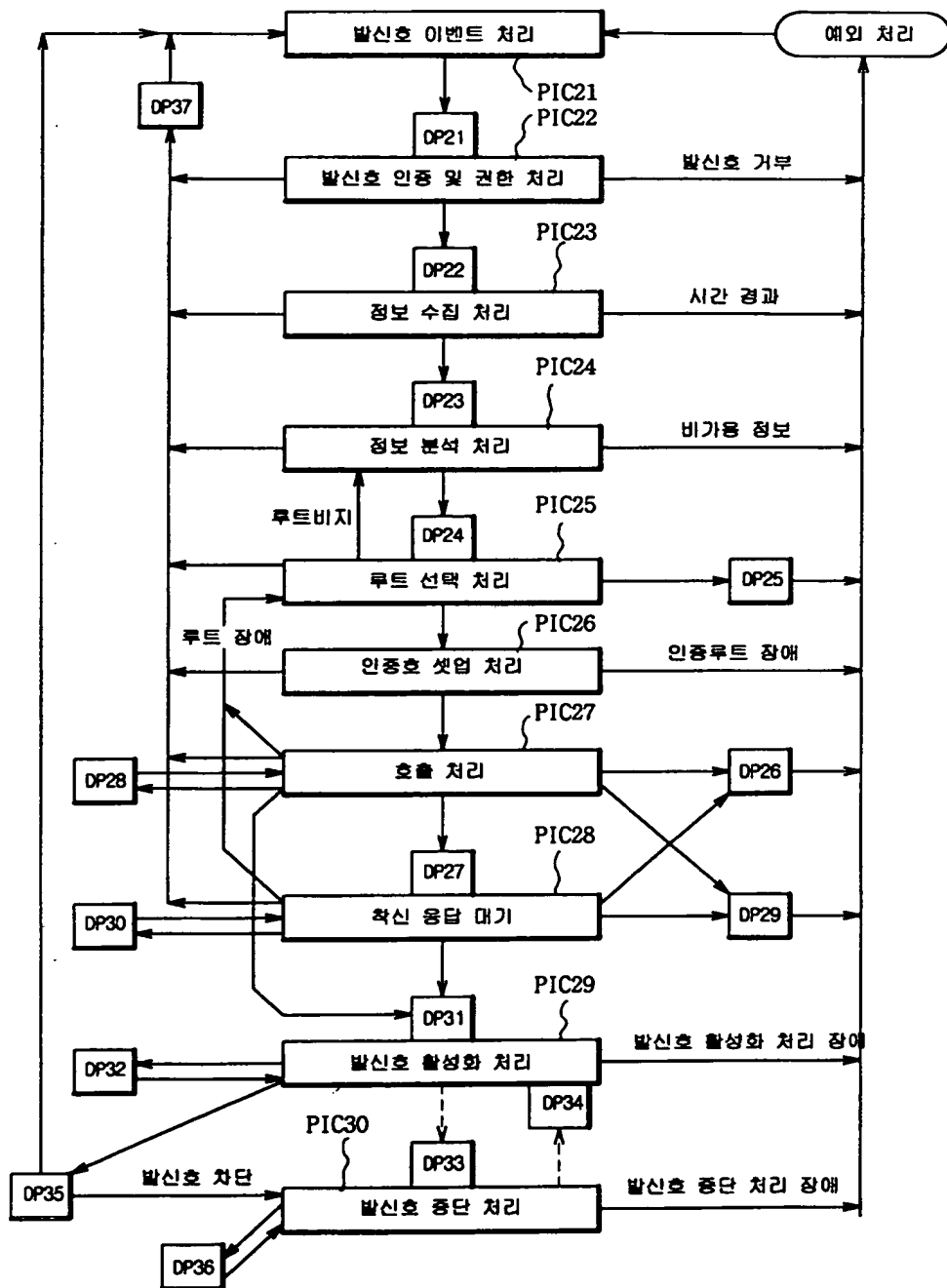
【도 1】



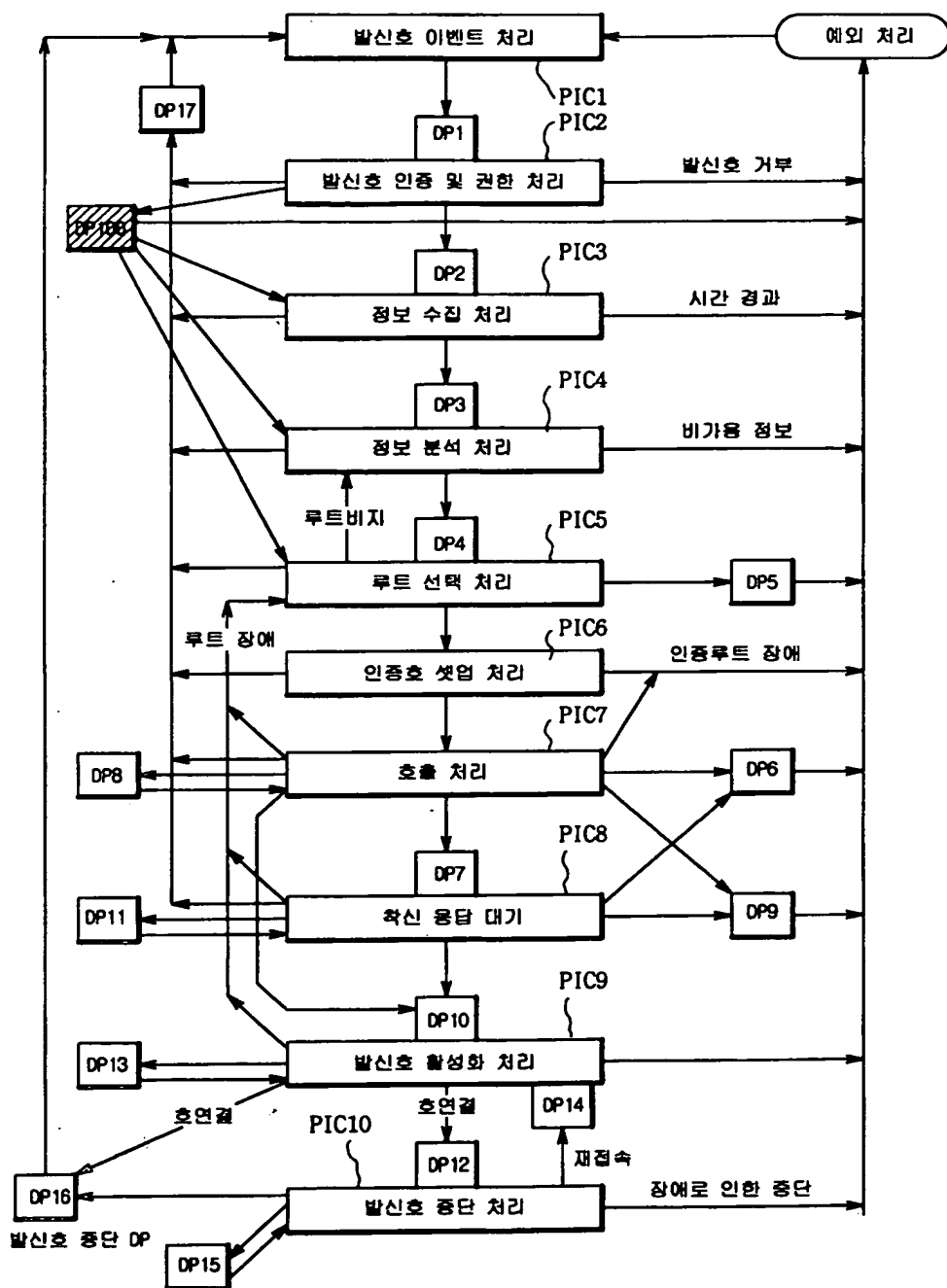
【도 2】



【도 3】



【도 5】



```

sequenceDiagram
    participant PIC21 as 발신호 이벤트 처리
    participant PIC22 as 발신호 인증 및 권한 처리
    participant PIC23 as 정보 수집 처리
    participant PIC24 as 정보 분석 처리
    participant PIC25 as 루트 선택 처리
    participant PIC26 as 인증호 셋업 처리
    participant PIC27 as 호출 처리
    participant PIC28 as 착신 응답 대기
    participant PIC29 as 발신호 활성화 처리
    participant PIC30 as 발신호 중단 처리

    PIC21 --> PIC22
    PIC22 --> PIC23
    PIC23 --> PIC24
    PIC24 --> PIC25
    PIC25 --> PIC26
    PIC26 --> PIC27
    PIC27 --> PIC28
    PIC28 --> PIC29
    PIC29 --> PIC30

    PIC22 --> DP21
    PIC23 --> DP22
    PIC24 --> DP23
    PIC25 --> DP24
    PIC26 --> DP25
    PIC27 --> DP26
    PIC28 --> DP27
    PIC29 --> DP31
    PIC30 --> DP33

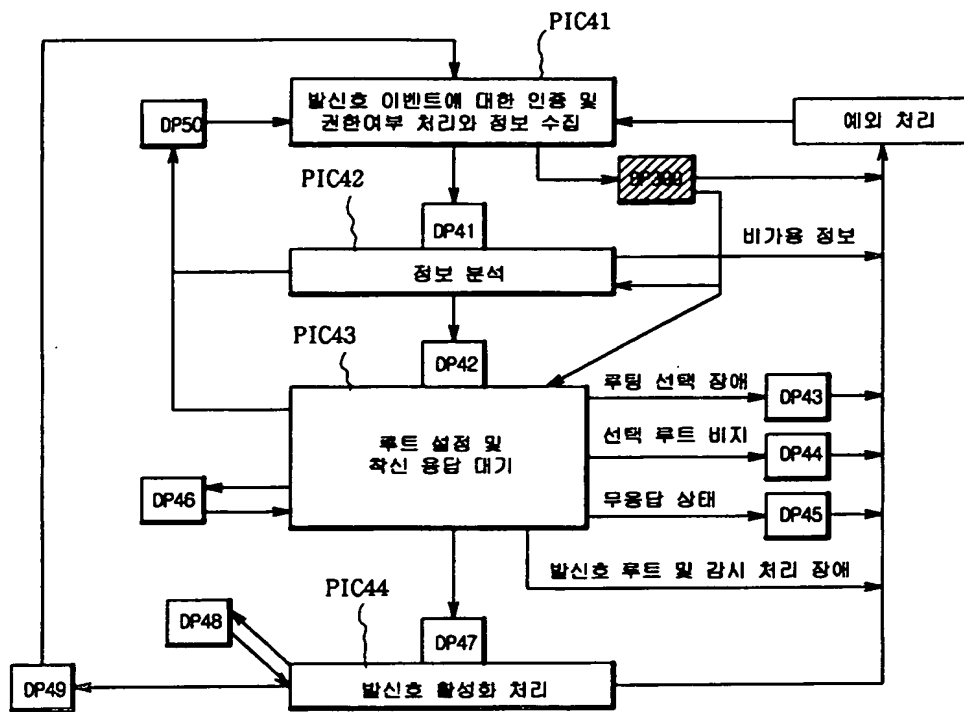
    DP21 --> PIC22
    DP22 --> PIC23
    DP23 --> PIC24
    DP24 --> PIC25
    DP25 --> PIC26
    DP26 --> PIC27
    DP27 --> PIC28
    DP31 --> PIC29
    DP33 --> PIC30

    PIC22 --> Out1[발신호 거부]
    PIC23 --> Out2[시간 경과]
    PIC24 --> Out3[비가용 정보]
    PIC25 --> Out4[루트 장애]
    PIC26 --> Out5[인증루트 장애]
    PIC27 --> Out6[호출 장애]
    PIC29 --> Out7[활성화 장애]
    PIC30 --> Out8[발신호 중단 처리 장애]

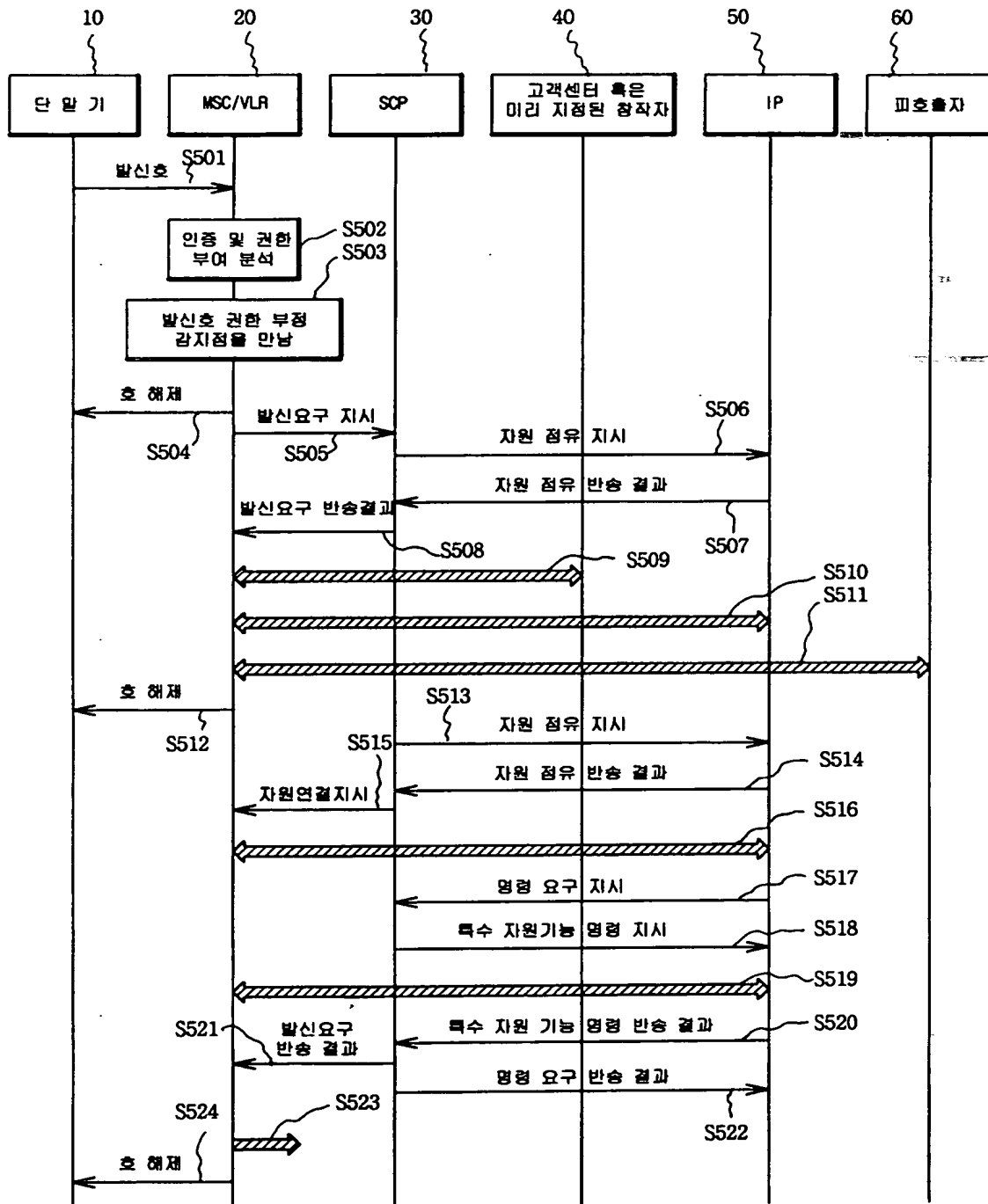
    Out1 --> PIC21
    Out2 --> PIC21
    Out3 --> PIC21
    Out4 --> PIC21
    Out5 --> PIC21
    Out6 --> PIC21
    Out7 --> PIC21
    Out8 --> PIC21

    PIC21 --> DP35[발신호 중단]
    DP35 --> PIC30
    
```

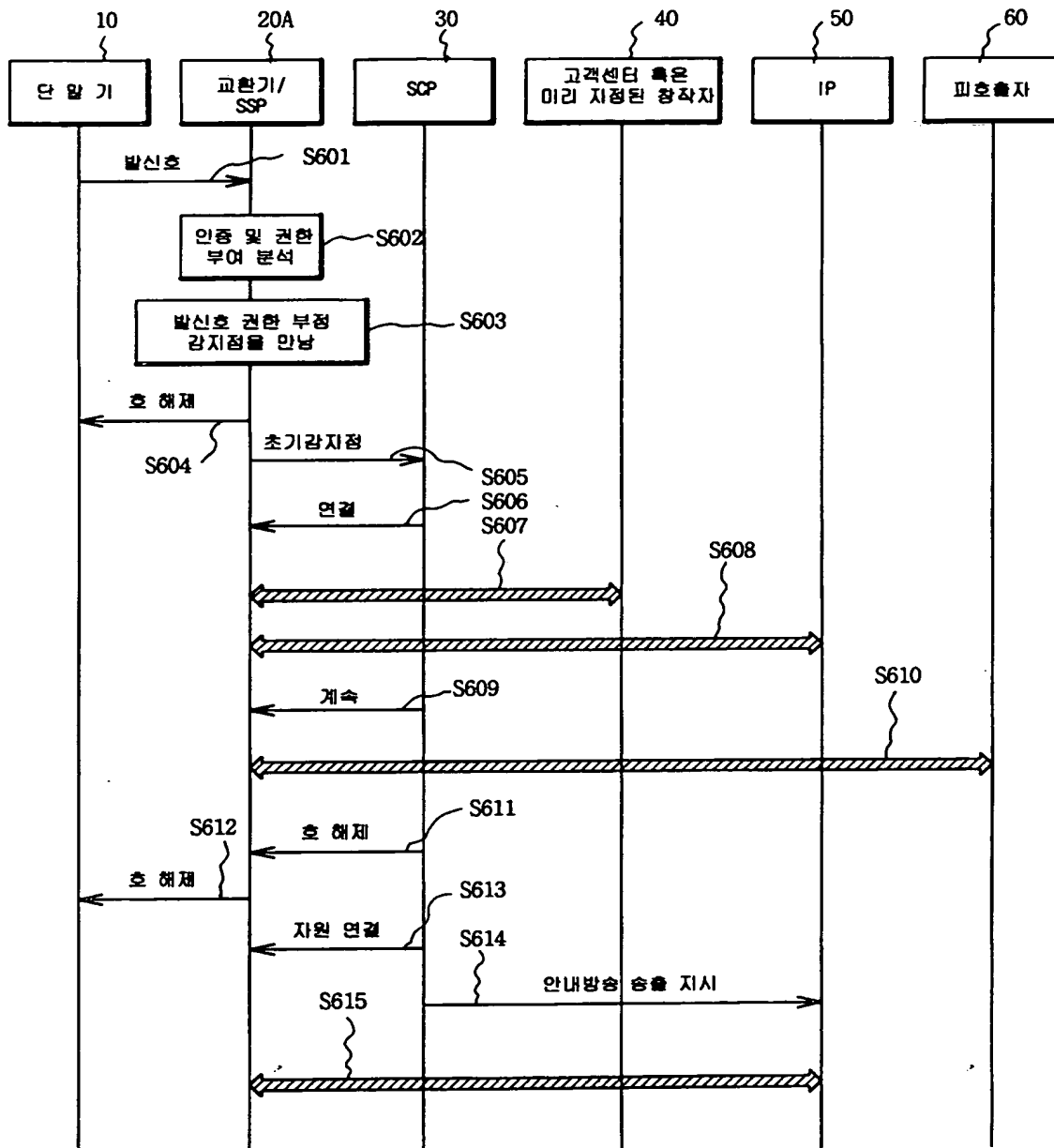
【도 7】



【도 8】



【도 9】



【도 10】

